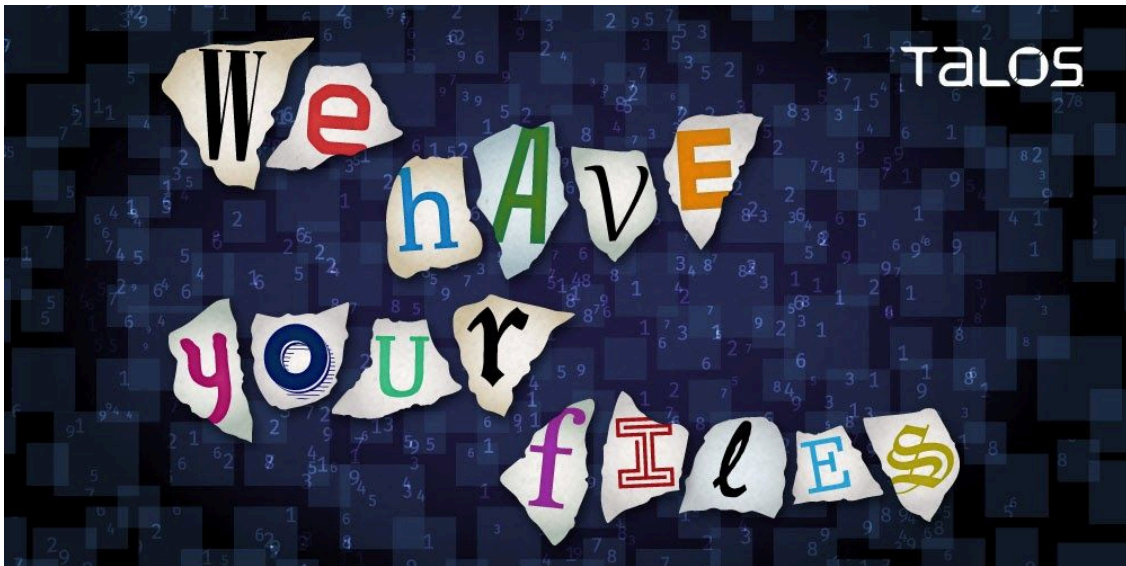


Nibiru ransomware variant decryptor

By William Largent

Published: 2020-11-17 · Archived: 2026-04-05 19:17:38 UTC



Tuesday, November 17, 2020 13:56

Weak encryption The Nibiru ransomware is a .NET-based malware family. It traverses directories in the local disks, encrypts files with Rijndael-256 and gives them a .Nibiru extension. Rijndael-256 is a secure encryption algorithm. However, Nibiru uses a hard-coded string "Nibiru" to compute the 32-byte key and 16-byte IV values. The decryptor program leverages this weakness to decrypt files encrypted by this variant.

Ransomware Nibiru ransomware is a poorly executed ransomware variant. It traverses directories and encrypts files with Rijndael-256. The files are given an extension, .Nibiru, after encryption. The ransomware targets numerous common file extensions but skips critical directories like Program Files, Windows and System Volume Information.

Extensions targeted by Nibiru:

.doc, .docx, .xls, .xlsx, .ppt, .pptx, .jpg, .jpeg, .png, .psd, .txt, .zip, .rar, .html, .php, .asp, .aspx, .mp4, .avi, .3gp, .wmv, .MOV, .mp3, .wav, .flac, .wma, .mov, .raw, .apk, .encrypt, .crypted, .ahok, .cs, .vb.

You can [download the decryptor](#) over at the Talos GitHub.

Example hash:

e0a681902f4f331582670e535a7d1eb3d6eff18d3fbed3ffd2433f898219576f

Source: <https://blog.talosintelligence.com/2020/11/Nibiru-ransomware.html>